Cryptography: The Science of Secrecy

Sergey Gorbunov

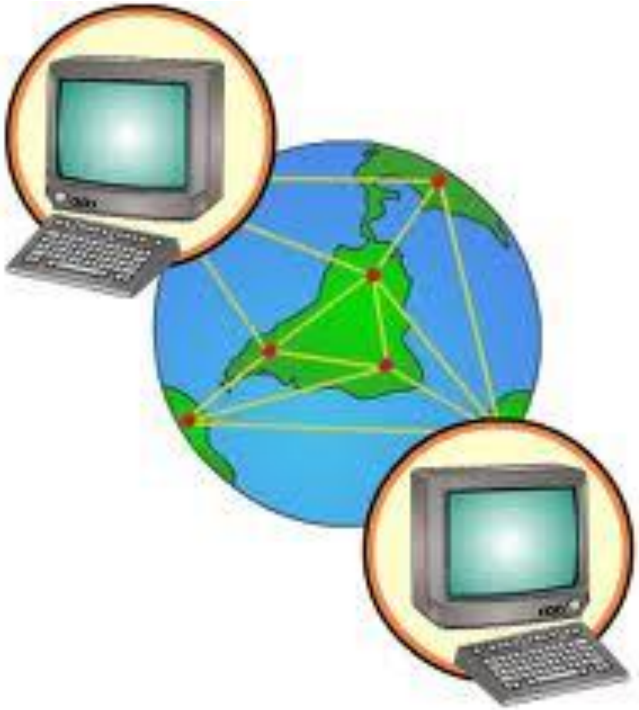
University of Toronto

"The urge to discover secrets is deeply ingrained in human nature"

-- John Chadwick

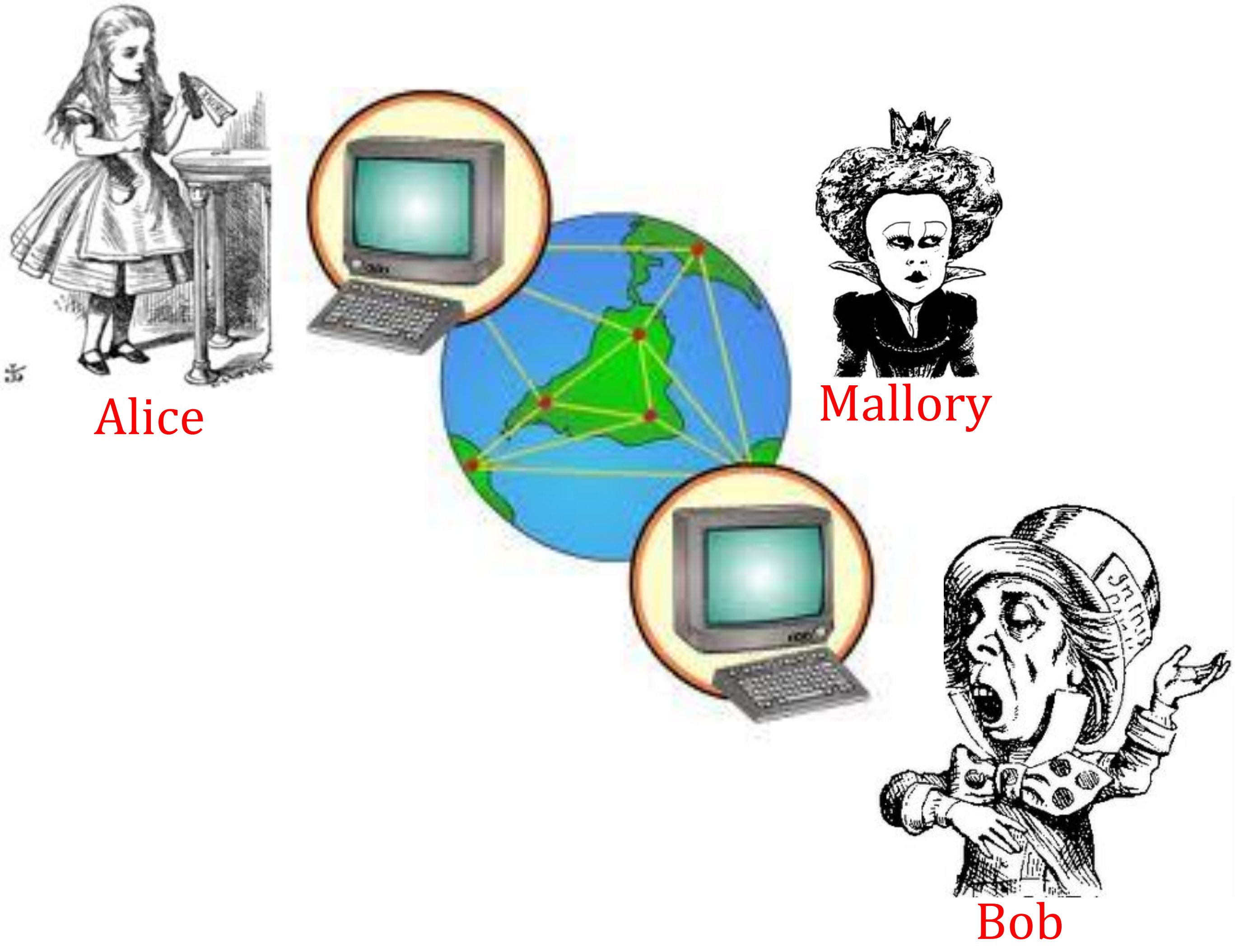
Communication in the "ideal world"

Alice



Bob

Communication in the “real world”



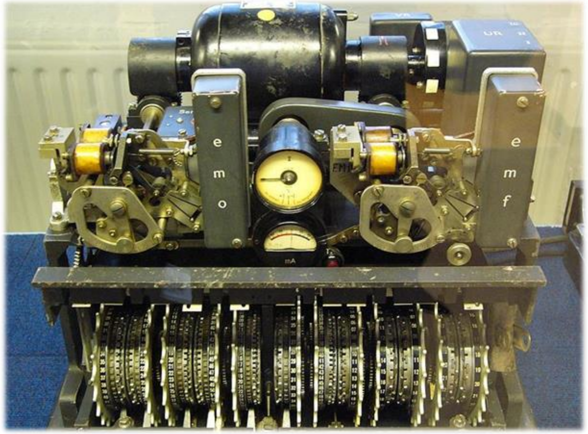
Alice

Mallory

Bob

What is cryptography?

- From Greek:
- κρυπτός -- "hidden, secret“
- γράφειν (*graphein*) -- "writing"



German Lorenz cipher machine, used in World War II

Cryptography offers:

- Privacy – hide messages from malicious users
- Authentication – verify “identity” of the speaker
- Data Integrity – validate that data hasn’t been changed in transition
- Secure Computation
- Zero Knowledge
- ….

Why is cryptography important?

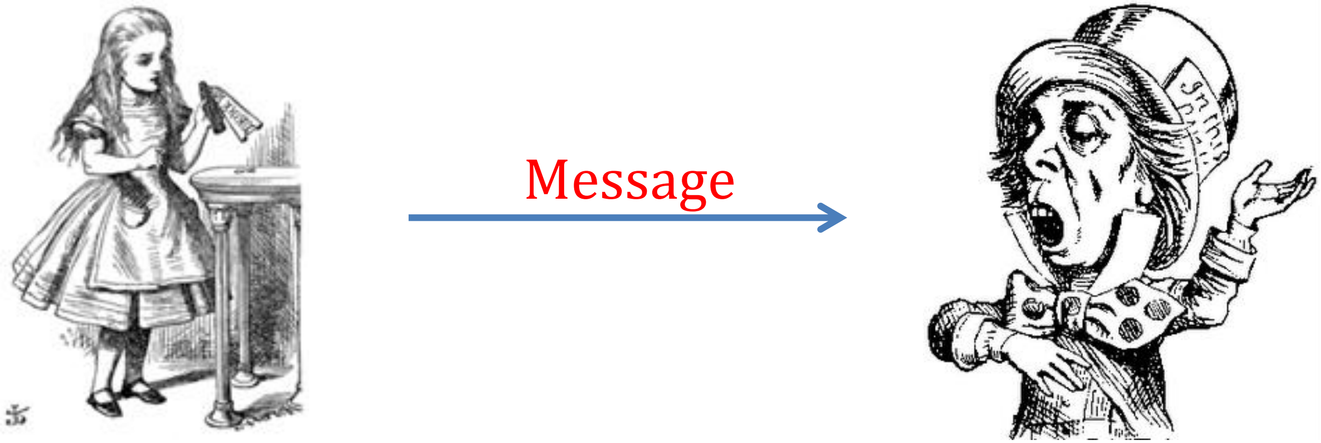
- Military
- Government
- Financial
- Education
- Health Care
- Personal Information

Real life threats

- “cyber attack could take down critical infrastructure and the power grid”, (computerworld.com)
- “The International Atomic Energy Agency acknowledged Tuesday that one of its servers had been hacked”, Nov 2012 (thestar.com)
- “PayPal, Symantec hacked as Anonymous begins November 5 hacking spree”, (zdnet.com)

Privacy

- *How can two people securely communicate over insecure communication media?*



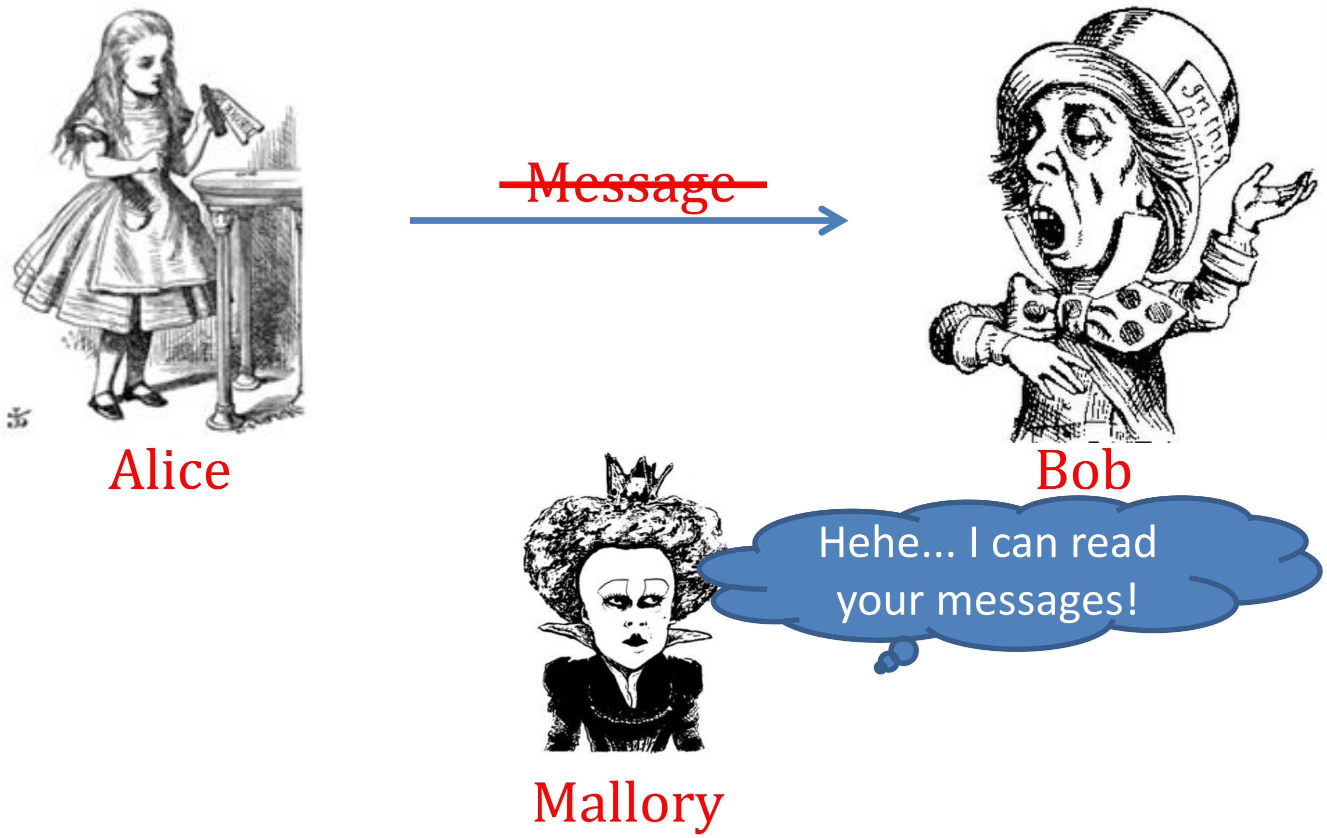
Message

Alice

Bob

Privacy

- *How can two people securely communicate over insecure communication media?*



~~Message~~

Alice

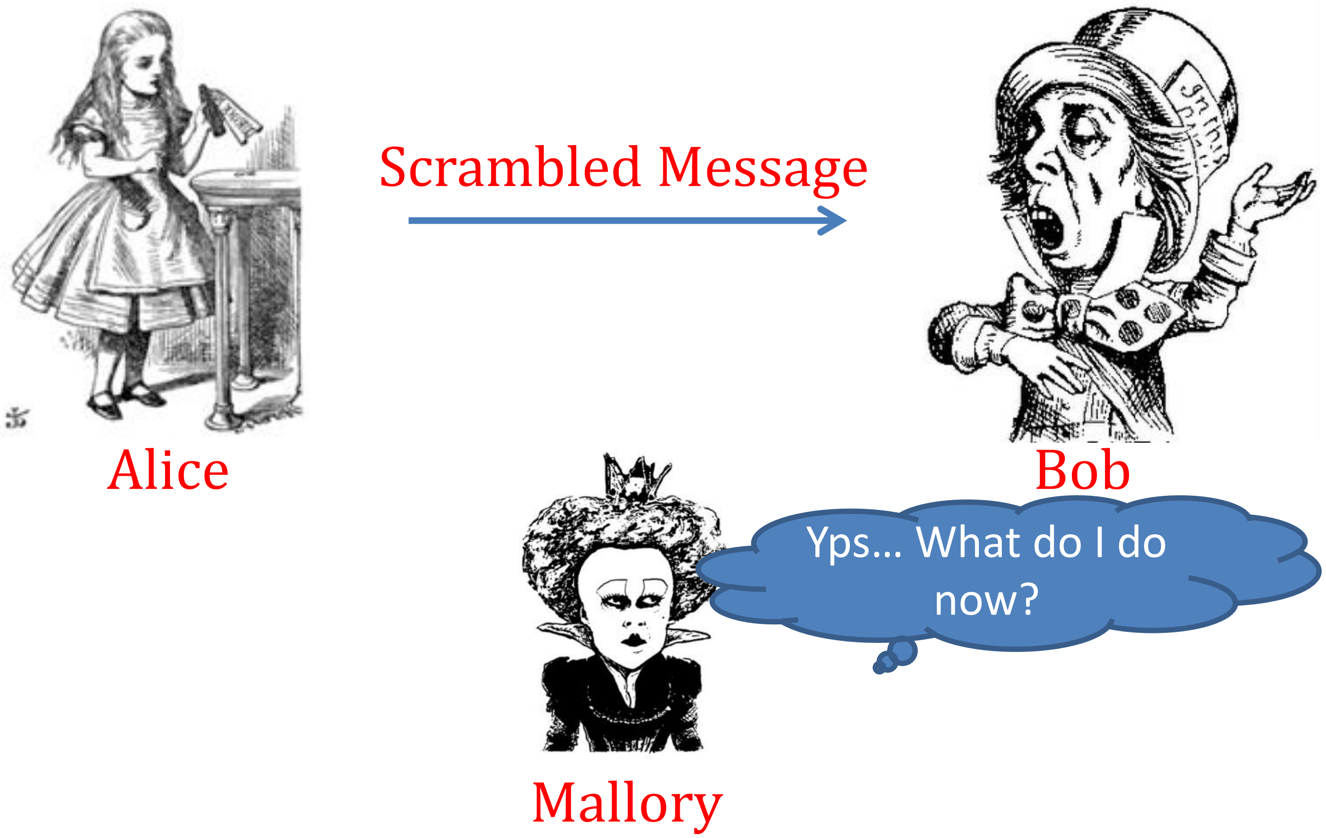
Bob

Hehe... I can read your messages!

Mallory

Privacy

- *How can two people securely communicate over insecure communication media?*



Scrambled Message

Alice

Bob

Mallory

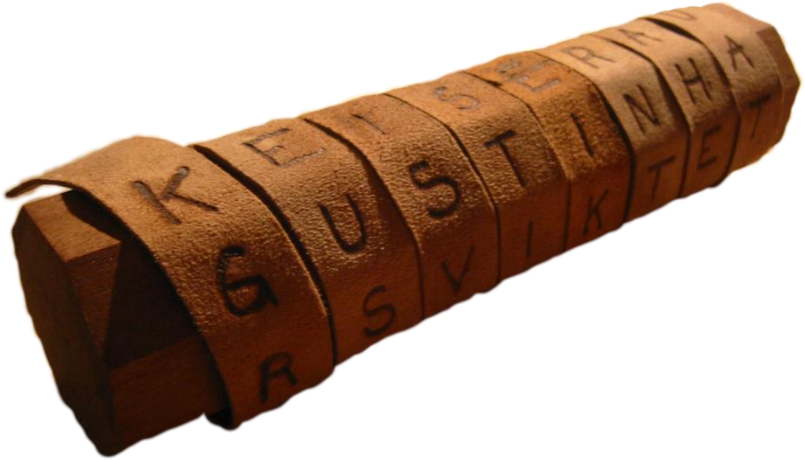
Yps… What do I do now?

Spartan *Scytale* Cipher

Cipher: is an algorithm used to scramble messages

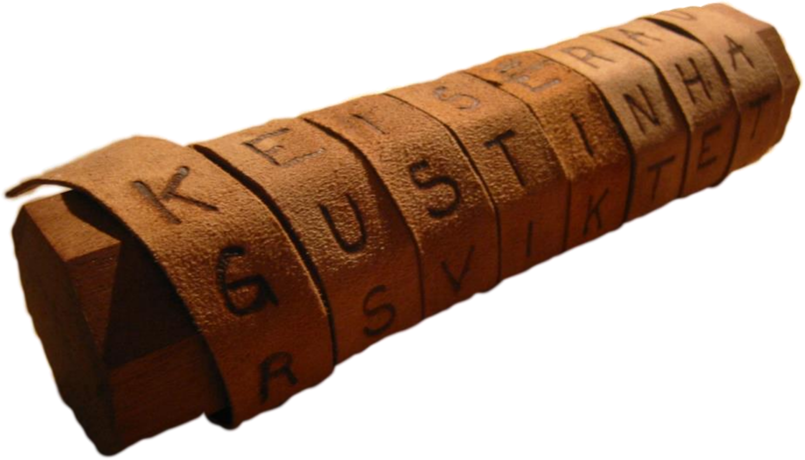
Spartan *Scytale* Cipher

- Dates back to the fifth century B.C.
- Greeks and Spartans used it to communicate during military campaigns



Spartan *Scytale* Cipher

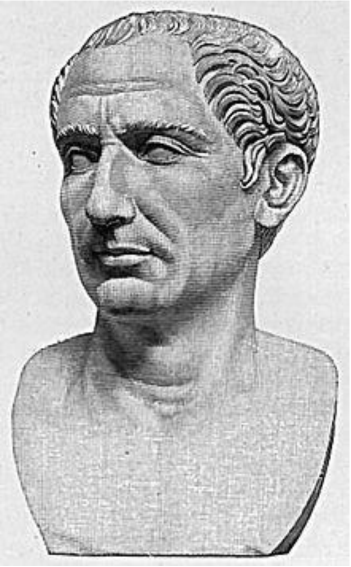
- Wooden stick around which a strip of leather is wrapped
- The sender writes the message along the length of the stick and unwinds the strip
- Known as a transposition cipher: letters are transposed in some order



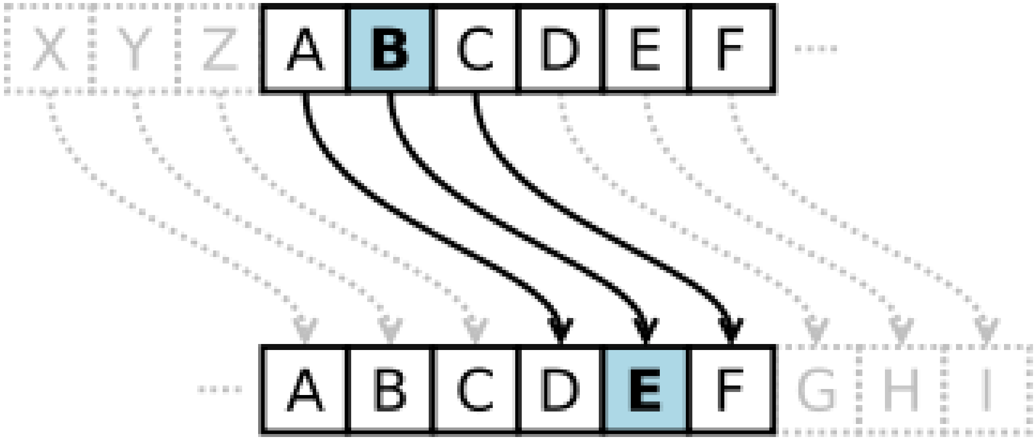
Spartan *Scytale* Cipher

- Easy to break: just find a stick with the same diameter
- In fact, we do not even need a stick to break it!
- Hypothesis: was also used an *authentication* mechanism

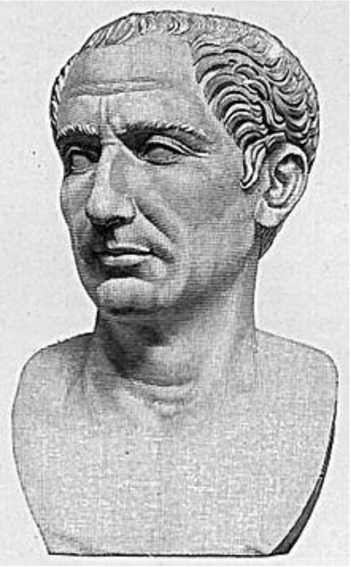
Caesar Cipher



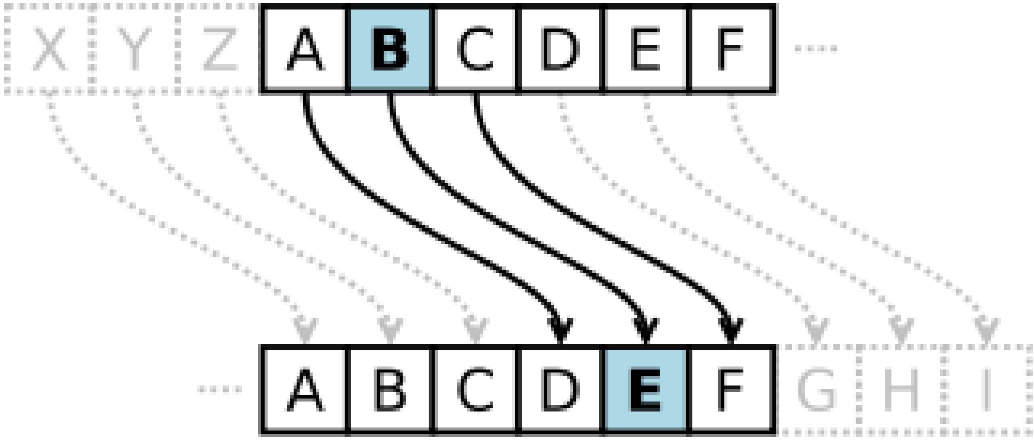
- Named after Julius Caesar (100 BC - 44 BC)
- Used to send scrambled messages of military significance to his generals



Caesar Cipher



- Each letter is replaced by a letter shifted by three positions in the alphabet
- Known as a substitution cipher



Caesar Cipher

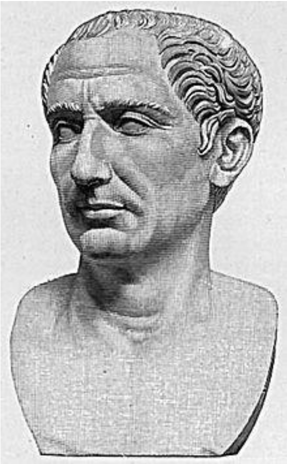
Encryption:

Message **ATTACK AT DAWN**

↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓

Shift by +3

Ciphertext **DWWDFN DW GDZQ**



DWWDFN DW GDZQ

Caesar Cipher

Decryption:

Ciphertext	`DWWDFN DW GDZQ`
Shift by -3	↓↓↓↓↓↓ ↓↓ ↓↓↓↓
Message	`ATTACK AT DAWN`

Caesar Cipher

Encryption:

Message **ATTACK AT DAWN**

↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓

Shift by +3

Ciphertext **DWWDFN DW GDZQ**

Shift by a random number in $\{1,2,3, \dots, 26\}$

Caesar Cipher

Encryption:

Message ATTACK AT DAWN

↓↓↓↓↓↓ ↓↓ ↓↓↓↓

Shift by +3

Ciphertext DWWDFN DW GDZQ

- Easy to break without even knowing the key!
- How?

Substitution Cipher

Encryption:

- Substitute characters of the message with another character
- A key is the permutation table

Decryption:

- Reverse the substitutions

a	b	c	d	e	f	g	h	i	j	k	l	m
M	I	B	A	U	P	E	G	Z	S	C	Y	W

n	o	p	q	r	s	t	u	v	w	x	y	z
Q	F	D	R	T	V	X	H	O	K	J	L	N

Substitution Cipher

Encrypt

Decrypt

Message: CRYPTO IS FUN

Ciphertext: BTLDWF ZV PHQ

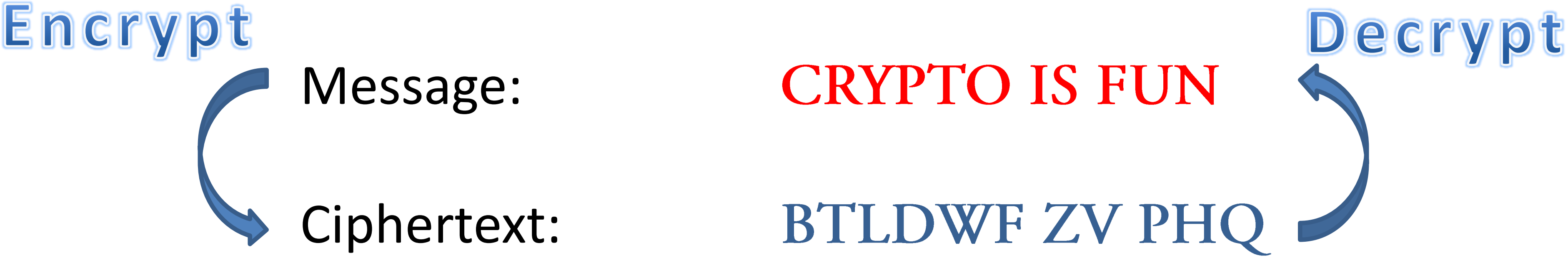
a	b	c	d	e	f	g	h	i	j	k	l	m
M	I	B	A	U	P	E	G	Z	S	C	Y	W

n	o	p	q	r	s	t	u	v	w	x	y	z
Q	F	D	R	T	V	X	H	O	K	J	L	N

Substitution Cipher

- How can we break this cipher without the key?
- Number of possible keys is

$$26 * 25 * 24 * \ \ldots \ * 1 = 26! \ \approx$$
400 million million million million



Encrypt

Decrypt

Message: CRYPTO IS FUN

Ciphertext: BTLDWF ZV PHQ

Substitution Cipher

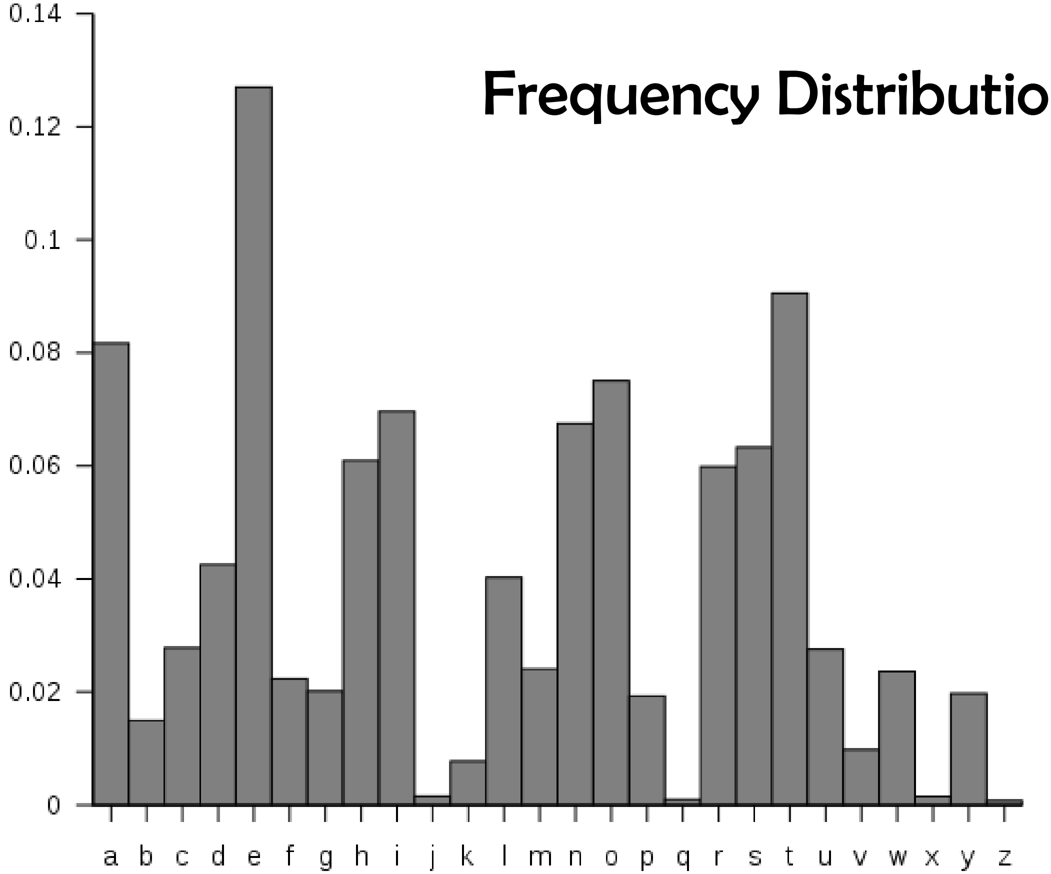
- English language has certain “properties” that are preserved in the ciphertext
- Note, that each letter is substituted with the same letter each time!
- Hence, most frequent letter in English with also be the most frequent letter in the ciphertext

Encrypt

Decrypt

Message: CRYPTO IS FUN

Ciphertext: BTLDWF ZV PHQ



Frequency Distribution of English

Encrypt

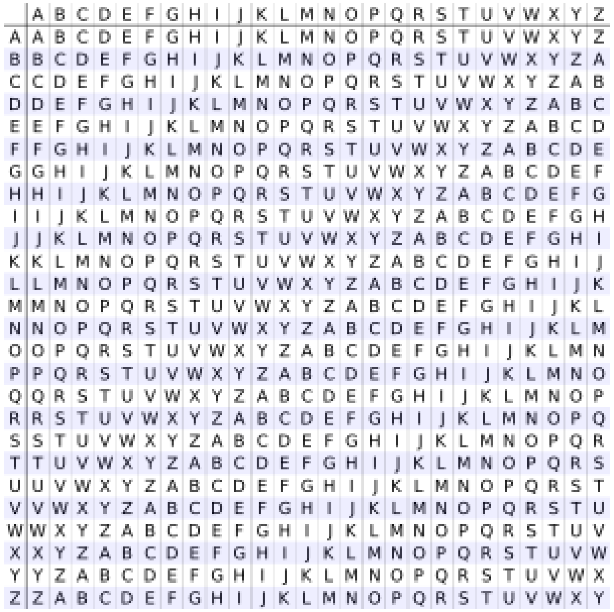
Message: CRYPTO IS FUN

Ciphertext: BTLDWF ZV PHQ

Decrypt

Polyalphabetic Ciphers

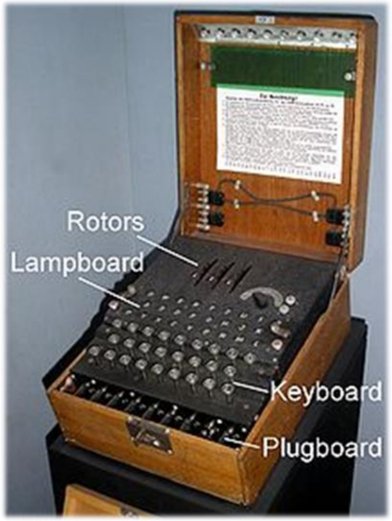
- “Multiple substitution ciphers”
- A key is a collection of substitution keys
- Originally presented by Giovan Battista Bellaso in his 1553 book
- Credit goes to 19th French Diplomat Blaise de Vigenère
- Does not fully hide the English Language Characteristics



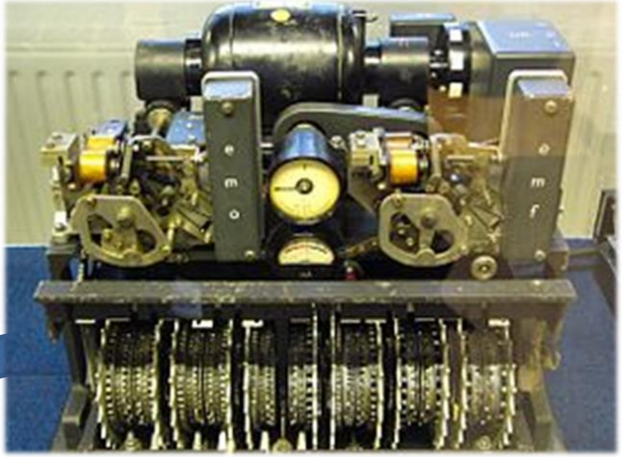
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Vigenère Cipher

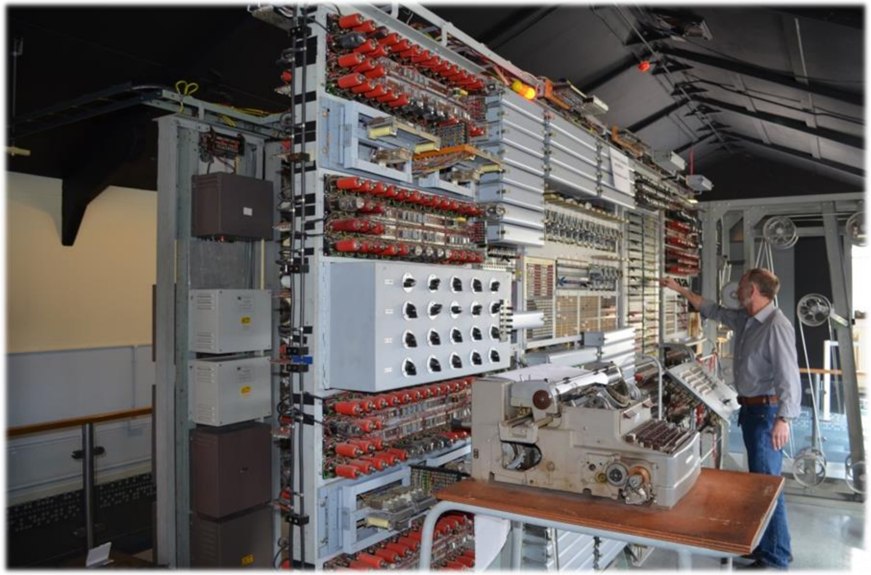
Polyalphabetic Ciphers



Enigma, WW2
Broken in 1932



Lorenz, WW2
Broken in 1942



Colossus computer

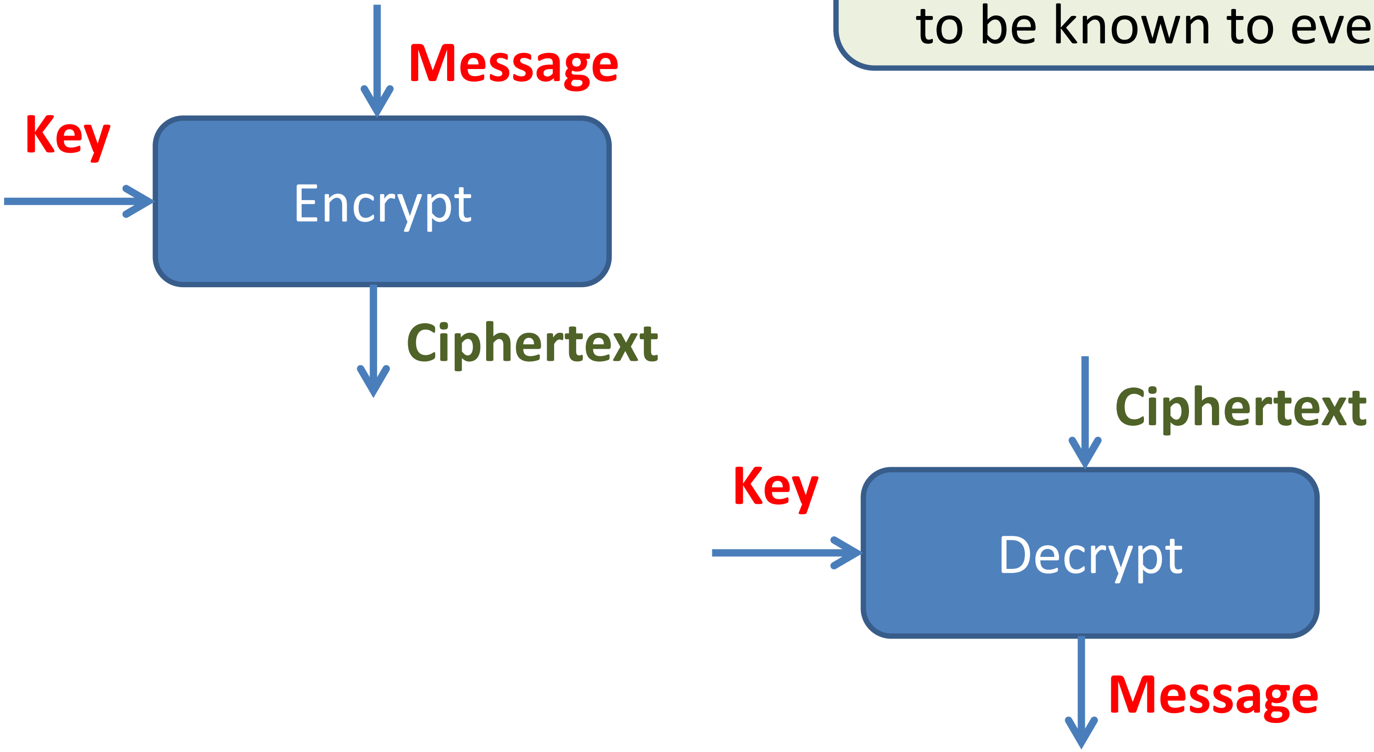
Finally, a wise man said:

“A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.”

-- Auguste Kerckhoffs

Encryption System

Both *Encrypt* and *Decrypt* algorithms are now assumed to be known to everyone!



Perfect "Symmetric" Encryption

Key = 0101101101

Key = 0101101101

Alice

Key: 0101101101

⊕

Msg: 1010001100

Bob

Ciphertext: 1111100001

"One-Time Pad is unbreakable" – Shannon 1949

Should you care about "perfect" privacy?

Key = 0101101101

Key = 0101101101

Alice

Key: 0101101101

$\oplus$

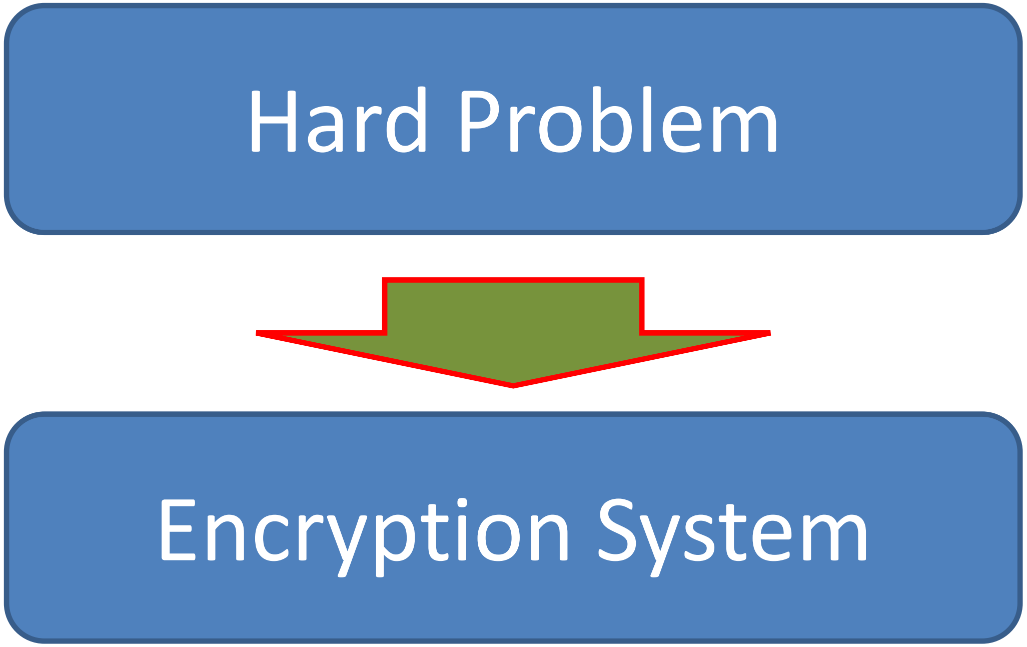
Msg: 1010001100

Ciphertext: 1111100001

Bob

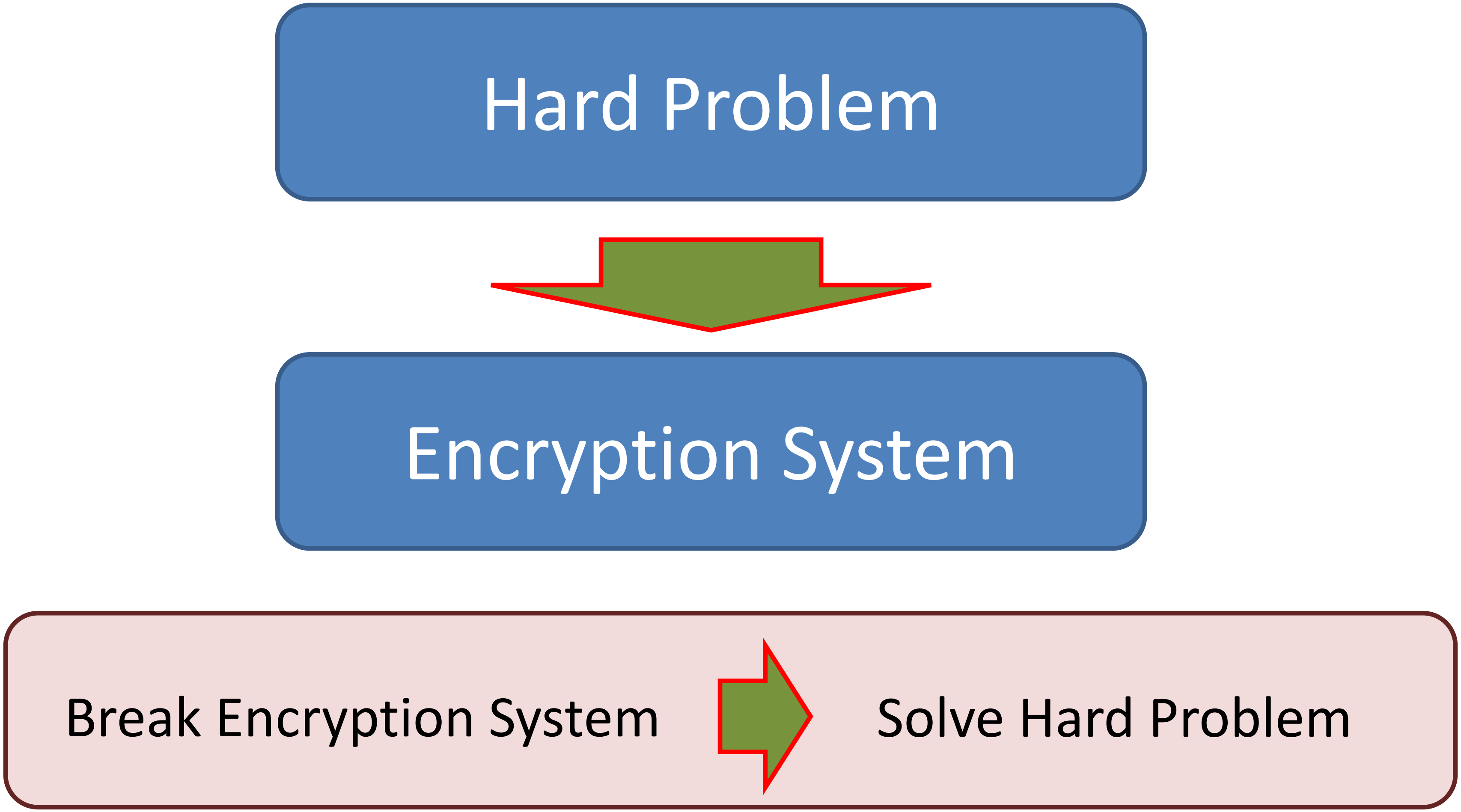
"One-Time Pad is unbreakable" – Shannon 1949

Should you care about “perfect” privacy? Maybe Not.


Hard Problem

Encryption System

Should you care about "perfect" privacy? Maybe Not.



Hard Problem

Encryption System

Break Encryption System

Solve Hard Problem

What are “hard” problems?

Multiplication

3499217945
5693345233 ×

VS

Factoring

Find **a, b** such that

a
b ×

32319562946749991681

What are “hard” problems?

Multiplication

3499217945
5693345233 ×

19922255806393806185

VS

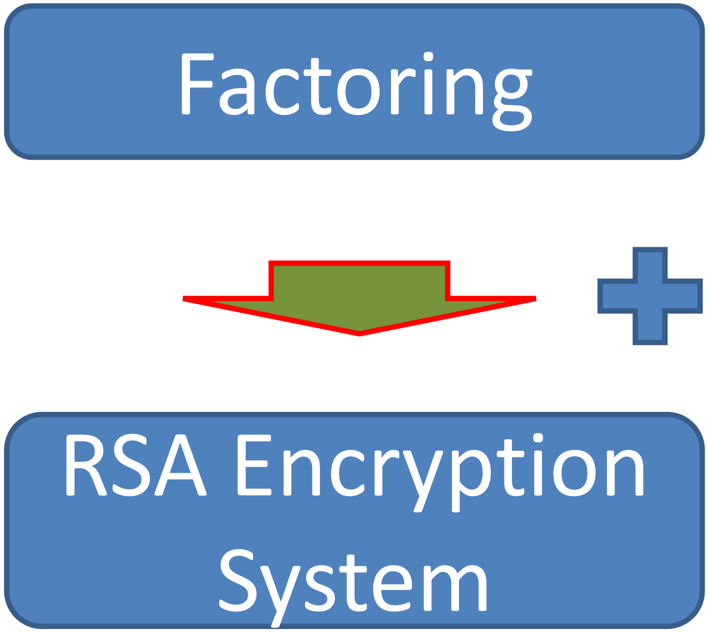
Factoring

Find **a, b** such that

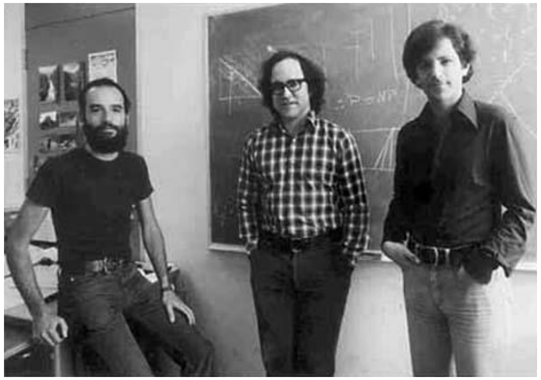
5915587277 ×
5463458053

32319562946749991681

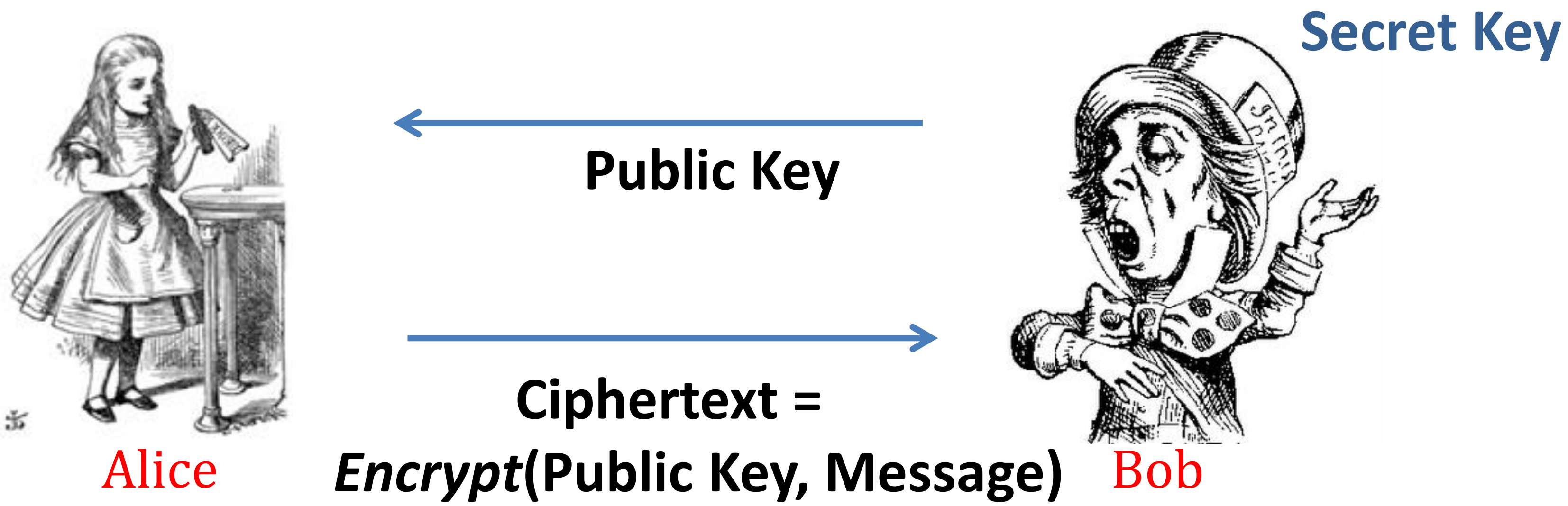
Should you care about "perfect" privacy? Maybe Not.


Factoring

RSA Encryption System


Shamir, Rivest and Adleman
(1978)

Public-Key Encryption (RSA)



Secret Key

Public Key

Ciphertext =
Encrypt(Public Key, Message)

Alice

Bob

Public-Key Encrypti

Only Bob can Decrypt the ciphertext using the Secret Key!

Secret Key

Alice

Public Key

Ciphertext = Encrypt(Public Key, Message)

Bob

ption (RSA)

Alice and Bob do not need to meet to establish the keys!

Alice

Secret Key

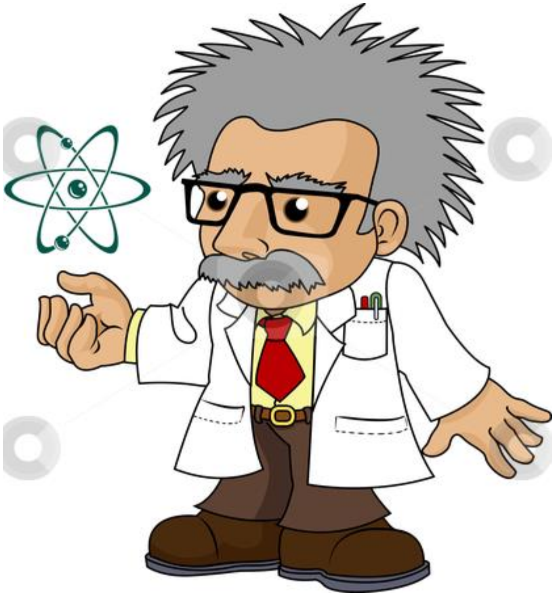
Bob

Public Key

Ciphertext = Encrypt(Public Key, Message)

Zero-Knowledge: Where is Waldo?

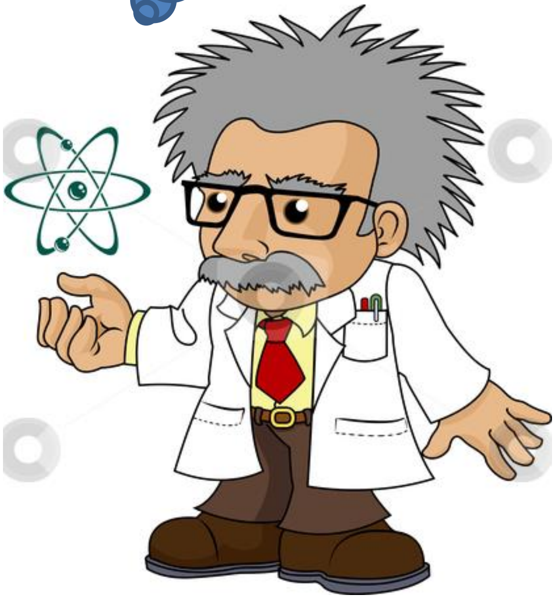
I know where Waldo is!



Zero-Knowledge: Where is Waldo?

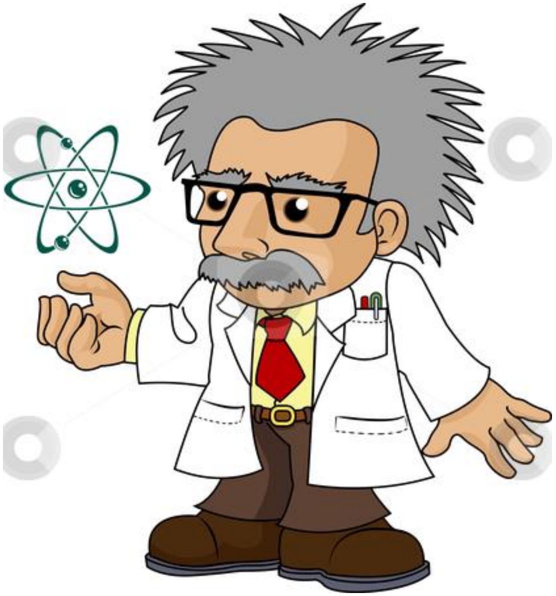
I know where Waldo is!

Do you know what a liar is?



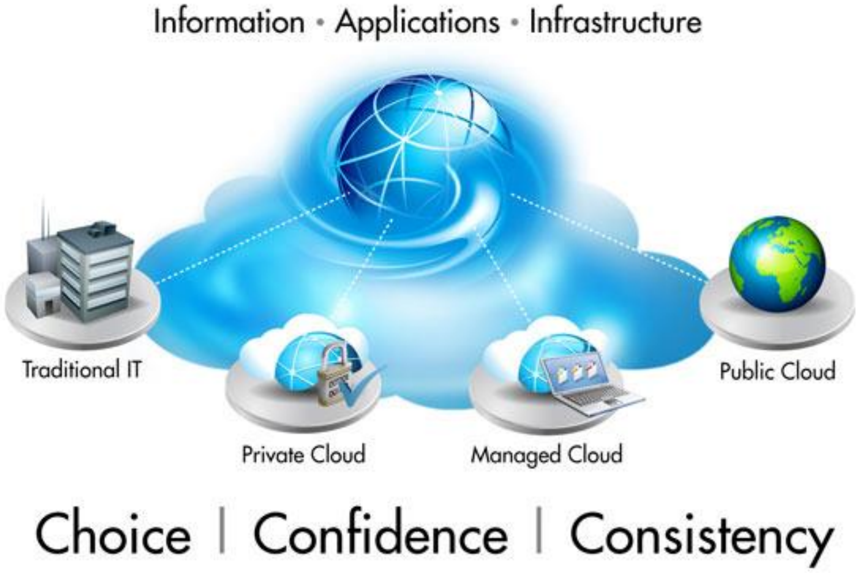
Zero-Knowledge: Where is Waldo?

How can I prove that I know where Waldo is without revealing his location?



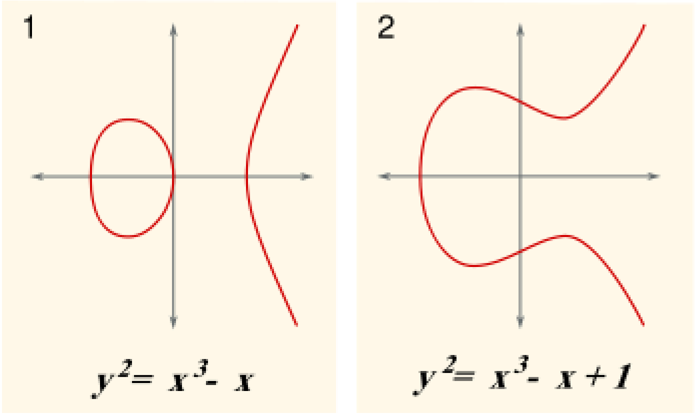
Today's Research

- Homomorphic Encryption
- Multi-Party Computation
- Digital Signatures
- Functional Encryption
- Hash Functions
- …


Information • Applications • Infrastructure
Traditional IT
Private Cloud
Managed Cloud
Public Cloud
Choice | Confidence | Consistency

Today’s Tools

Elliptic Curves

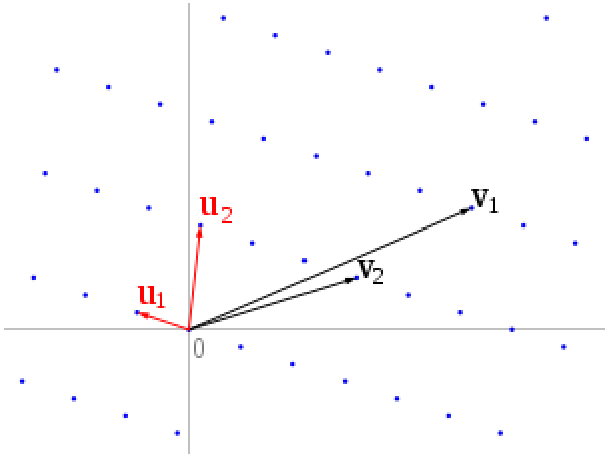


Number/Group Theory

$$m^e \pmod{n}$$

$$c^d \pmod{n}$$

Lattices



Thank you!